LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of creating a single sign-on role certificate using a PKI system, comprising:

accessing a PKI system, through a client platform, by a user in which a digital signature certificate has been previously created for the user and transmitting the digital signature certificate to the PKI system;

verifying the identity and validity of the user ~~through the PKI system~~ by accessing a directory using the digital signature certificate;

signaling the client platform to create a private/public key pair;

generating ~~a~~ the private/public key pair at the client platform and transmitting the public key of the private/public key pair to the PKI system from the client platform;

transmitting the public key to a domain certificate authority for signature; and

returning the public key to the ~~user~~client platform signed by the domain certificate authority, wherein the signed public key is operative as the single sign-on role certificate.

2. (Original) The method recited in claim 1, further comprising:

authenticating the user identity; and

verifying the user has authority to receive the public key.

3. (Original) The method recited in claim 2, further comprising:

delivering a password to the user through the mail to the user's home address;

accessing the PKI system by the user using the password; and

receiving the digital signature certificate.

4. (Original) The method recited in claim 3, wherein the digital signature may be used for both signatures and encryption.

5. (Original) The method recited in claim 1, wherein the verifying the identity and validity of the user by PKI system by accessing a directory using the digital signature certificate further comprises;

verifying that the digital signature certificate has not been revoked; and

verifying that the user is still a member of the organization.

6. (Original) The method recited in claim 5, further comprising:

storing the public key signed by the domain certificate authority in a hardware token, smart card, a computer, a magnetic strip card, or other storage device.

7. (Original) The method recited in claim 6, further comprising:

accessing a foreign computer network not associated with the PKI system using the public key signed by the domain certificate authority.

8. (Currently Amended) A computer program embodied on a computer readable medium and executable by a computer to create a single sign-on role certificate using a PKI system, comprising:

~~accessing a PKI system by a user in which a digital signature certificate has been previously created for the user and transmitting the digital signature certificate to the PKI system;~~

receiving a digital certificate associated with a user from a client platform;

verifying the identity and validity of the user ~~by PKI system~~ by accessing a directory using the digital signature certificate;

signaling the client platform to create a private/public key pair;

~~generating private/public key pair and transmitting the public key to the PKI system;~~

receiving the public key of the private/public key pair from the client platform;

transmitting the public key to a domain certificate authority for signature; ~~and~~

receiving a signed public key from the domain certificate authority; and

returning the signed public key to the ~~user~~ client platform signed by the domain certificate authority, wherein the signed public key is operative as the single sign-on role certificate.

9. (Original) The computer program recited in claim 8, further comprising:

authenticating the user identity; and

verifying the user has authority to receive the public key.

10. (Canceled)

11. (Original) The computer program recited in claim 10, wherein the digital signature certificate may be used for both signatures and encryption.

12. (Original) The computer program recited in claim 8, wherein verifying the identity and validity of the user by PKI system by accessing a directory using the digital signature certificate further comprises;

verifying that the digital signature certificate has not been revoked; and

verifying that the user is still a member of the organization.

13. (Canceled)

14. (Original) The computer program recited in claim 13, further comprising:

accessing a foreign computer network not associated with the PKI system using the public key signed by the domain certificate authority.

15. (Currently Amended) A method of creating a single sign-on role certificate using a PKI system, comprising:

creating a digital signature certificate verifying the identity of a user and authority of the user to obtain the digital signature certificate;

delivering a password to the user through the mail to the user's home address;

accessing a PKI system, through a client platform, by the user using the password;

receiving the digital signature certificate from the PKI system;

accessing a PKI system, through the client platform, by a user using the digital signature certificate;

verifying the validity of the user by ~~PKI system~~ accessing a directory using the digital signature certificate;

signaling the client platform to create a private/public key pair;

generating the private/public key pair and transmitting the public key of the private/public key pair to the PKI system from the client platform;

transmitting the public key to a domain certificate authority for signature; and

returning the public key to the ~~user~~client platform signed by the domain certificate authority, wherein the signed public key is operative as the single sign-on role certificate.

16. (Original) The method recited in claim 15, wherein the digital signature certificate is used for both signatures and encryption.

17. (Original) The method recited in claim 15, wherein verifying the identity and validity of the user by PKI system by accessing a directory using the digital signature certificate further comprises;

verifying that the digital signature certificate has not been revoked; and

verifying that the user is still a member of the organization.

18. (Original) The method recited in claim 17, further comprising:

storing the public key signed by the domain certificate authority in a hardware token, smart card, a computer, a magnetic strip card, or other storage device.

19 (Original) The method recited in claim 18, further comprising:

accessing a foreign computer network not associated with the PKI system using the public key signed by the domain certificate authority.